The SUCI-AKA Authentication Protocol for 5G Systems

Geir M. Køien

Department of Microsystems,
University of South-Eastern Norway,
Campus Vestfold, Norway
geir.koien@usn.no

Abstract

Security is a fundamental requirement for all digital systems. In this paper we propose a new entity authentication protocol, which we call the SUCI-AKA protocol. In contrast to the existing 5G-AKA protocol, it will provide online mutual entity authentication. A central design criteria has been to provide a solution which minimizes the system impact and avoids hard breaks with existing schemes. The SUCI-AKA protocol is largely based on the new 5G scheme for subscriber privacy, and integrates it with the existing 5G-AKA entity authentication protocol in a novel way. This provides scope for accommodating both credible subscriber privacy and online mutual entity authentication.

1 Introduction

1.1 Background and Context

1.1.1 Access Security in Mobile Systems

Security was recognized as a requirement already during the first generation, and successively the security has improved over the generation. Much of the access security hinges on the "Authentication and Key Agreement" (AKA) protocols. These are challenge-response protocols, with a pre-shared secret, K and the $IMSI$ subscriber identifier as the base credentials. The schemes rely on pseudo-random challenges, and responses generated by message authentication code (MAC), using K as the key. The AKA protocols include three principal parties.

- *The User Equipment (UE).* A proxy for the subscriber.
- *The Home Network (HN).* An anchor point.
- *The Serving Network (SN).* Where the UE is being "logged" on.

The UE consists of a subscription identity module(SIM or USIM), and a mobile equipment (ME) device. The HN is where the permanent subscriber data is stored. The SN may belong to the same operator as does the HN, or it may belong to some other network. If the SN does not belong to the same network as the HN, then the SN is said to be a Visiting Network (VN). In this paper, there is no distinction whether the SN belongs to the HN or a VN.

1.1.2 The Mobile System Generations

We have 5 generations of mobile system, with an approximately 10 year interval between them. With respect to access security we have:

- *1G - 1981: Analogue speech, digital call setup. These systems had almost no security.*
- *2G - 1991: All-digital, and with basic access security capabilities.*

  GSM was the prominent 2G system. The GSM-AKA protocol provided subscriber authentication, and GSM had over-the-air 64-bit encryption.

- *3G - 2001: All-digital, and with more advanced access security procedures.*

  UMTS was the prominent 3G system. The UMTS-AKA protocol provided (offline) authenticated challenges and subscriber authentication. UMTS had confidentiality protection (128-bit key) and integrity protection for the signalling (128-bit key, 32-bit mac).

- *4G - 2010: All-IP systems, providing mobile broadband as a basic service.*

  The LTE systems (several versions) has an EPS-AKA protocol that provides (offline) authenticated challenges and authentication of the UE. An EPS-AKA run sets up a security context with a 256-bit master key (K_{ASME}). Sessions key are 128-bit wide.

- *5G - 2020: All-IP system. A lot of new designs in the system architecture.*

  The 5G system provides a redesigned core network architecture and new radio (NR) system. The 5G-AKA protocol and the associated key hierarchy is slightly more advanced than the EPS-AKA counterpart. The (main) anchor key is called K_{AUSF}. The biggest news with 5G access security is the Subscription Concealed Identifier (SUCI) scheme.

1.1.3 Trust Relationship

The trust relationships for access security in mobile systems are basically as follows.

- *UE-HN: Primary trust relationship.*

  Legally binding agreement by means of the subscription contract. The HN issues identifiers and security credential to the UE. The lifetime is defined by the subscription.

- *HN-VN: Primary trust relationship.*

  A legally binding roaming agreement covers this case. It may involve roaming brokers mediating the VN-HN relationship. The lifetime is defined by the roaming agreement.

- *UE-VN: Secondary (derived) relationship.*

  This relationship is established during the AKA run (mediated by the HN). The lifetime of the relationship is limited to the lifetime of security context established by the AKA protocol run. It may be renewed by new re-running the AKA protocol.

Note that an SN may be a VN, but it may also belong to the same entity as controls the HN. The access security protocols are designed for the generic (roaming) case, where the SN belongs to a VN. The terms SN and VN is often used interchangeably.

1.2 Prior Works

For the previous generations (2G-4G), there is a body of papers that propose various enhancements to the AKA protocols [1, 2, 3, 4] (there are many more). Some of these papers also address the need for incorporating subscriber privacy. There are (yet) comparatively few works concerning 5G security. There are some papers analyzing the 5G access security, and there are a few that provided suggestions for what 5G should have been (some prior to the standardization and some later). Examples include [5, 6, 7, 8]. However, few of the proposals in the academic literature pay much attention to the design context of the AKA protocols. That is, the proposals tend to break with existing schemes in ways that are not likely to be acceptable, or where the additional gains are not likely to be considered worthwhile. We thus believe that our SUCI-AKA protocol proposal are novel in that the aim for minimal design impact, yet aim to provide real advantages.

1.3 Outline of the Paper

Section 1 is the introductory part of the paper. Section 2 defines the design criteria and the security requirements for the SUCI-AKA protocol. Section 3 outlines the 5G access security schemes. Section 4 provides a short analysis of the Subscription Concealed Identifier (SUCI) scheme and the 5G-AKA protocol. Section 5 outlines and describes the SUCI-AKA protocol. It also contains a brief analysis of the protocol. Section 6 provides a summary and a conclusion.

2 High-Level Requirements

A substantial part of the contribution of this paper is concerned with understanding the context of the target system.

2.1 Scope

We are proposing changes to a system that is widely deployed and with billions of users. One had then better avoid changes that break with existing designs, unless there is no other way.

2.2 Design Criteria

We approach the design of the SUCI-AKA protocol with the following design strategy:

- *Efficiency is important, but it is not an end-goal.*
  A full entity authentication run is not a frequent event. The executing entities will have considerably processing powers. Efficiency considerations that were meaningful in previous generations, are often irrelevant in a 5G context.
- *Minimal Impact on the Existing Procedures and System Architecture.*
  Design, implementation and deployment costs must be contained.
- *Avoid impact at the Serving Network.*
  There must be changes to the HN and the UE to provide online mutual authentication. If changes to the SN can be avoided, it will much easier to introduce the new protocol.
- *Minimize impact on the USIM.*
  It is very costly to replace the USIM's. It is not only the hardware costs of the UICC hardware, on which the USIM resides, but the logistics and management of issuing and deploying the physical cards. We will strive to avoid changes to the USIM.
- *Build on existing functionality when appropriate.*
  In UMTS one decided that one should keep security mechanisms (from 2G) that were needed and robust (Section 4 in [9]). We concur with this idea.

2.3 Security Requirements

The security requirements captured here are complementary to the existing set of requirements. That is, the requirements are provided in the context of existing 5G systems.

1. *Provision of online mutual entity authentication between the UE and the HN.*
   The UE-HN trust relationship must be confirmed. The 5G-AKA protocol only provides indirect authentication of the HN. The UE will know that the HN issued the challenge, but cannot know if the HN is still present. There is thus a need for online mutual entity

authentication between the UE and the HN. The need is particularly pronounced for initial registration at a new SN.

2. *The SUCI scheme is to be retained.*
   Subscriber identity privacy and location privacy are essential features, and the SUCI scheme provides this. Thus, we want to retain the basics of the SUCI scheme.
3. *No changes to the key hierarchy.*
   The key hierarchy is deeply integrated with the system architecture. Still, it is considered within scope to change the derivation of the anchor key material (the K_{AUSF} key).
4. *Perfect Forward Secrecy (PFS) for the anchor key.*
   The K_{AUSF} anchor key shall have the PFS property. This will not provide PFS for the key hierarchy per se, but key reconstruction will be limited to the anchor key.
5. *The SUCI-AKA protocol must be able to co-exist with the 5G-AKA protocol.*
   The SUCI-AKA protocol is primarily intended for initial registration with a new SN.

3 Access Security in 5G Systems

This section contains brief descriptions of the 5G access security procedures. We limit ourselves to the identity presentation, entity authentication procedures and the generation of security context key material (or keys). We will strive to keep the discussion generic, and avoid system specific details whenever possible. As mentioned, the 5G system is designed to be compatible with the 4G system, but not with 2G or 3G systems. However, the 4G and 5G AKA protocols are derived from the UMTS-AKA protocol, and the USIM is essentially still a 3G USIM. In addition, the basic subscriber identifiers ($IMSI$ and $TMSI$) originate with 2G (GSM).

3.1 Subscriber Identification and Associated Identifiers

3.1.1 The International Mobile Subscriber Identity (IMSI)

The $IMSI$ identifier is described in Section 2 in TS 23.003 [10]. It is consists of a Mobile Country Code (MCC), a Mobile Network Code (MNC) and the Mobile Subscriber Identification Number (MSIN). The $IMSI$ is globally unique and is permanently stored on the UE and at the HN.

$$IMSI = MCC||MNC||MSIN$$

The $IMSI$ is one of the possible instantiations of the SUPI identifer (see below).

3.1.2 The Temporary Mobile Subscriber Identifier (TMSI)

The $TMSI$ is a 2G and 3G temporary identifier. It has local significance at the SN, and is a 32-bit wide unstructured variable. It is assigned to the UE when encryption has commenced. Subsequently, the $TMSI$ is use in plain-text form as the UE identifier. This provides for a measure of subscriber privacy, with the caveat that the $IMSI$ would have to be presented in plain-text over-the-air prior to assignment of $TMSI$. For $TMSI$ to be useful with respect to privacy, it must be unlinkable. There are no standardized requirements to enforce this.

3.1.3 The Globally Unique Temporary UE Identity (GUTI)

There are $GUTI$s defined for 4G and for 5G (Section 2 in TS 23.003 [10]). The $GUTI$s are compound identifiers, which encapsulate a $TMSI$ with additional addressing information. The $M\text{-}TMSI$ (4G) and $5G\text{-}TMSI$ are similar to the 2G/3G $TMSI$. All $TMSI$s are 32-bit wide.

3.1.4 The Subscription Permanent Identifier (SUPI)

The $SUPI$ is described in Section 2 in TS 23.003 [10]. The globally unique $SUPI$ is either an $IMSI$, a Network Access Identifier (NAI), a Global Cable Identifier or a Global Line Identifier. An exposed $SUPI$ will compromise identity privacy, as well as permitting unsolicited positioning and tracking.

3.1.5 The Subscription Concealed Identifier (SUCI)

The $SUCI$, see Figure 1, is the concealed correspondent identifier to the $SUPI$. It is described

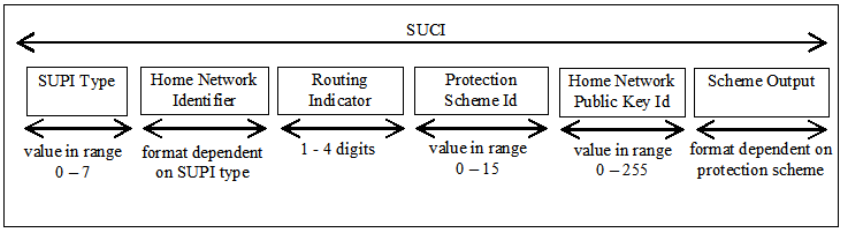

Figure 2.2B-1: Structure of SUCI

Figure 1: The SUCI (Transposed from TS 23.003)

in Section 2 in TS 23.003 [10]. It includes various parameters, including a HN identifier, a HN public key, a protection scheme identifier and the concealed $SUPI$ (`Scheme Output`).

3.2 Subscriber Privacy Prior to 5G

Prior to 5G, the only mechanisms was the above mentioned $TMSI$ scheme. The $TMSI$ scheme suffers from the fact that the UE initially have to provide the $IMSI$ in plain-text over-the-air. Furthermore, the SN can request the UE to provide the $IMSI$ (in plain-text).

3.3 Identity Presentation with the SUCI Scheme

The initial identity presentation in 2G-4G is necessarily by means of the permanent $IMSI$ identifier. With 5G, the initial identity presentation to a SN is by means the $SUCI$ identifier. Subsequent identification is preferably by means of the $5G{-}GUTI$ identifier As depicted in Figure 1, the $SUCI$ includes a HN identifier, a HN public key, a protection scheme identifier and the concealed $SUPI$ (`Scheme Output`).

3.3.1 The use of ECIES in the SUCI Scheme

The Elliptic Curve Integrated Encryption Scheme (ECIES) is the main building block of the SUCI scheme. ECIES is a hybrid scheme and configurable cryptographic framework. It includes an elliptic-curve Diffie–Hellman (DH) exchange, symmetric key derivation and symmetric key encryption- and message authentication. A useful survey of ECIES can be found in [11].

The SUCI scheme is depicted in Figure 2 (UE viewpoint). The UE must have obtained a suitable EC public key from the HN prior to the exchange. The sequence starts with the UE generating a corresponding ephemeral key-pair. This key-pair is used to compute a DH

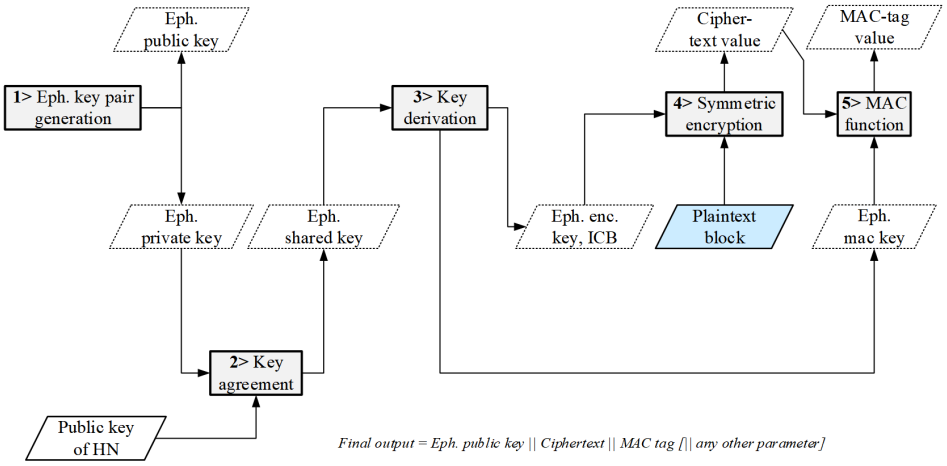

Figure C.3.2-1: Encryption based on ECIES at UE

Figure 2: The SUCI Procedure (at the UE) (Transposed from TS 33.501, Annex C.3)

secret, which is then used to derive a confidentiality key and an integrity key. These are used to protect the message (the $SUPI$). The protected message and the UE's ephemeral public key is forwarded to the HN (there may be other data included in the message). The HN, using the received public key, computes the DH secret, and decrypts and checks the $SUPI$.

3.4 The UMTS-AKA Protocol

The UMTS-AKA protocol was devised for use with 3G networks. The UMTS-AKA challenge-response scheme is essentially embedded in the 5G-AKA protocol. This complicates the 5G-AKA protocol, but also allows the USIM to be retained.

The UMTS-AKA protocol provides authentication of the UE and an authenticated challenge [12]. Prior to running the challenge-response procedure, the SN will request the HN for an authentication vector (AV). The HN may provide up to 5 AVs in one exchange. We have:

```
AV = {RAND: 128-bit pseudo-random challenge
      AUTN: 64-bit Authentication Token. AUTN: (AMF,SQN, MAC-A)
      CK:   128-bit confidentiality key
      IK:   128-bit integrity key
      XRES: 64-bit signed response value}
```

The $AUTN$ consists of an authentication management field (AMF), a sequence number (SQN) and a $MAC{-}A$ value to verify the authenticity of the challenge. The UE will terminate the AKA run if the $MAC{-}A$ check fails, while providing failure indication to the SN. The UE will trigger a re-synchronization procedure if SQN is invalid.

The UMTS-AKA protocol (abridged and simplified):

1. UE→SN: RequestAccess($IMSI$)
2. SN→HN: RequestAV($IMSI$)
3. HN→SN: ProvideAV($n \cdot AV$)
4. SN→UE: Challenge($RAND, AUTN$)

5. UE: Check the $MAC\text{-}A$. Verify validity of SQN.
6. UE→SN: Response(RES)

The SN considers the authentication successful if ($RES = XRES$). The prefix X denotes *expected* value). The only difference between an X and a non-X response is the vantage point. The HN is never informed of successful outcome, but may optionally be informed if authentication fails. The identifier in step 1 may be a $TMSI$. The are several cryptographic functions defined for the UMTS-AKA protocol (see TS 33.105 (cryptographic requirements) and TS 33.102 (security architecture) [13, 12]) The most important functions are:

- $f1_K(RAND, SQN, AMF) \rightarrow MAC{-}A$
- $f2_K(RAND) \rightarrow RES$
- $f3_K(RAND) \rightarrow CK$
- $f4_K(RAND) \rightarrow IK$

There is a lot more to be said about UMTS access security. The interested reader is referred to [14, 15] for more on UMTS access security.

3.5 The 5G-AKA Protocol

The primary 5G security specifications is TS 33.501 "Security architecture and procedures for 5G System" [16]. TS 33.501 is not the most eloquent of documents, and we advocate having a look at the tutorial paper "3GPP 5G Security" [17]. The 5G architecture is defined in TS 23.002 [18]. The subscription authentication shared secret K is stored at the UE and HN. We note that the 5G-AKA protocol encapsulate the basics of the UMTS-AKA challenge-response. That also means that the UMTS-AKA functions are part of the 5G-AKA protocol. There is a 5G Authentication Vector (AV), which is defined as follows:

$$5G{-}AV = \{RAND, AUTN, K_{AUSF}, XRES^*\}$$

The $RAND$ is the (pseudo) random challenge from the HN to the UE, and the $AUTN$ is an authentication token. These are essentially the same as for the UMTS-AKA protocol. The UMTS-AKA protocol had a RES element, which was the response to the challenge. In 5G, the RES is not used directly. Instead, an $XRES^*$ is derived from RES. The derivation is defined in TS 33.501 (in Annex A.4 in [16]). There are several similar key derivations defined in Annex A in TS 33.501. The cryptographic function used is HMAC-SHA256 (see Annex B.2 in TS 33.220 [19]).

$$A.4 : Res^*_{(CK||IK)}(FC, P0, L0, P1, L1, P2, L2) \tag{1}$$

Where:

- FC: Function code (0x6B)
- $P0$: SN-name, and $L0$ is the length
- $P1$: $RAND$, and $L1$ is the length
- $P2$: RES (or $XRES$), and $L2$ is the length

The 256-bit wide K_{AUSF} is derived from the CK and IK keys, with K as the controlling key (see Annex A.2 in TS 33.501 [16]). The CK, IK key pair originate with the UMTS-AKA protocol. The K_{AUSF} is an anchor key (HN/UE-side). There are also a K_{SEAF} anchor key (SN/UE-side) (Annex A.6 in TS 33.501 [16]). The anchor keys are key-deriving keys, and they belong to a corresponding security context. Figure 3 shows an outline of the 5G-AKA protocol with the main network functions.

Note that:

- AUSF is the security anchor network function within the HN.
- SEAF is the security anchor function at the SN. AMF is an associated SN function.
- UDM, ARPF and SIDF are HN functions that aid the AUSF in 5G-AKA processing.

The baseline 5G-AKA protocol is fairly similar to the 4G EPS-AKA protocol. The 5G key hierarchy and the security contexts are different from their 4G counterpart, but the overall structure is the same. However, the 5G-AKA does have some significant new features:

- The HN is online during 5G-AKA execution.
- Both the SN and the HN verifies the 5G-AKA response from the UE.
- The HN only processes authentication requests from authorized networks.
- The HN does not provide K_{SEAF} or $SUPI$ to the SN until the UE been authenticated.
- All authentication results are logged at the HN (by the UDM network function).
- An "Anti-Biding down Between Architectures (ABBA)" feature (not discussed further).

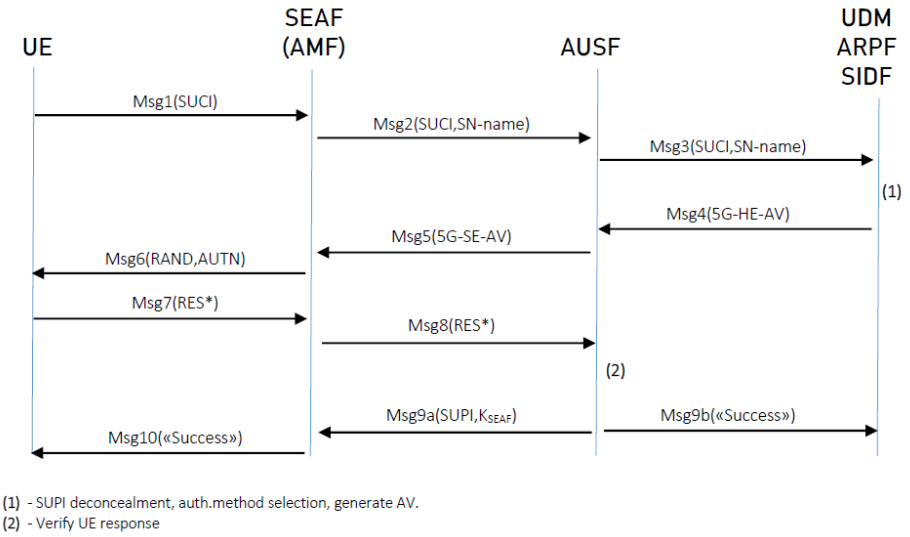

Figure 3: Outline of 5G-AKA (w/SUCI))

3.5.1 The 5G Security Contexts and Key Hierarchy

The 5G key hierarchy is larger than the 4G key hierarchy. There are HN-UE specific security contexts in addition to various SN-related security contexts. We shall not go into the details of these security contexts or the associated keys, suffice to say that whole hierarchy is based on the (CK, IK) keys. That is, the foundation of 5G-AKA is still based on the UMTS cryptographic functions. The basis for the CK, IK key-pair is still the 128-bit pre-shared symmetric key K. This is a pragmatic solution, and it avoid the costly logistics in replacing billions of already distributed USIM card. Please refer to Section 6.2 in TS 33.501 [16] for a complete account.

3.5.2 Alice-Bob outline of the 5G-AKA Protocol

The following is an outline of the 5G-AKA protocol. The UE identifier is either a $SUCI$ or a $5G{-}GUTI$. We have simplified the exchange to enhance readability. We focus on the principals, but also need to take the network functions into account.

— **Initial phase: Initialization and Identity presentation**

1. UE: Generate $SUCI$.
   UE→SN: N1-message($SUCI$)
2. SN→HN: UEAuth_AuthRequest($SUCI$, SN-name)
3. HN: De-conceal $SUPI$. Select auth.method.

— **Main phase: The 5G-AKA sequence**

4. HN.UDM/ARPF: Generate $5G{-}AV$.
5. HN: UDM/ARPF→AUSF: UEAuth_GetResponse($5G{-}AV$,$SUPI$)
6. HN.AUSF:
   - $A.5(RAND, XRES^*) \rightarrow HXRES^*$ (Annex A.5 [16])
   - $A.6_{K_{AUSF}}(FC, SN{-}name, Len(SN{-}name) \rightarrow K_{SEAF}$ (Annex A.6 [16])
7. HN.AUSF→SN.SEAF: UEAuth_AuthResponse($RAND, AUTN, HXRES^*$)
8. SN.SEAF→UE: NAS_AuthReq($RAND, AUTN$)
9. UE: Compute "UMTS-AKA" part at USIM. ME computes non-3G parts.
   - UE.USIM: Verify $AUTN$ ("UMTS-AKA": AV authenticity and sequence validity).
   - UE.ME: Compute RES and RES^*.
10. UE→SN.SEAF: NAS_AuthResp(RES^*)
11. SN.SEAF: Verify UE response
    - $A.5(RAND, RES^*) \rightarrow HRES^*$.
    - UE is deemed to be authenticated by SN.SEAF iff ($HRES^* = RES^*$).
12. SN.SEAF→HN.KAUSF: UEAuth_AuthRequest(RES^*)
13. HN.AUSF: Successful UE authentication iff: ($RES^* = XRES^*$). Log the result.
14. HN.AUSF→SN.SEAF: UEAuth_AuthResponse($SUPI, K_{SEAF}$)

Subsequent to the 5G-AKA sequence, the SEAF and the AUSF has the necessary security context key material (K_{SEAF} and ($KAUSF$) respectively), and both has assurance of the UE. The UE, on the other hand, cannot truly know that the HN is online. It has assurance that the challenge was computed by the HN, and it has assurance that the challenge was computed for use with the specific SN.

4 Brief Analysis of SUCI and the 5G-AKA Protocol

The following is a brief analysis of the SUCI scheme and the 5G-AKA protocol. We relate the analysis to the requirements identified in Section 2.

4.1 Properties of the SUCI Scheme

The use of ECIES in the SUCI scheme provides confidentiality protection of the $SUPI$. The ECIES construction is well-understood and in widespread use. The HN will be able to de-conceal the $SUPI$, and the $SUPI$ is not disclosed to the SN until after successful 5G-AKA verification. The SUCI scheme is needed, and it is clearly also an effective solution. Note that the SN plays no part in the SUCI scheme except to forward the $SUCI$.

Use of the SUCI scheme is a matter of policy (decided by the HN). While SUCI is mandatory for use, the UE may optionally use the NULL scheme, which renders the effort futile. Extended use of 5G-GUTI would also weaken the privacy.

4.2 Improvements in the 5G-AKA Protocol

The 5G-AKA provides several useful improvements over the EPS-AKA, most of which is listed in Section 3.5. We have not fully explained the 5G-AKA response scheme, with two-hashed variant of the RES. This scheme permits improved verification of the UE towards the HN and the SN. However, these improvements does not address UE beliefs in the HN or the SN.

4.3 Concerns with the 5G-AKA Protocol

4.3.1 Omissions in the 5G-AKA Protocol

The lack of explicit mutual entity authentication between the UE and the HN is an obvious omission. Likewise, the lack of the perfect forward secrecy property. That is, it is possible to regenerate the anchor key, K_{AUSF} (and the associated key hierarchy), if an entity has obtained the authentication secret K.

4.3.2 Complexity Concerns

We have only skimmed the surface of all the 5G-AKA protocol. And, we have not even mentioned the 4G-5G interworking parts, with context mapping, etc. Then there is the key hierarchy, which is also quite complex. The key derivations are mostly trivial per se, but the overall complexity is daunting. One may therefore argue that the 5G-AKA protocol is unnecessarily complex, and that it is difficult to verify that the design is correct. While this is a valid concern, we are even more concerned about the implementations of the 5G-AKA protocol. Minor misunderstandings could all too easily lead to implementation errors.

5 The SUCI-AKA Protocol Proposal

The SUCI-AKA protocol is proposed in the context defined by the 5G system architecture, and by the constraints of the design criteria and security requirements defined in section 2.

5.1 The Integration of SUCI in the SUCI-AKA Protocol

We want to utilize the SUCI scheme to provide a SUCI-AKA challenge mechanism for us. Specifically, we require:

- The UE must be able to configure $SUCI$ to indicate the SUCI-AKA protocol.
- The UE need to provide a challenge to the HN.
- The HN/UE must be able to use the EC DH secret as the basis for K_{AUSF}
- The existing SUCI scheme functionality should not be changed.

5.1.1 Using the Protection Scheme Identifier to Indicate the SUCI-AKA Protocol

The UE will need to indicate to the HN that it wants to trigger a SUCI-AKA protocol run. One possible way to do this is to used the existing ECIES profile parameter. Annex C in TS 33.501 [16] describes the current ECIES profiles (Null, A or B). The profile used is encoded in the $SUCI$ in the `Protection Scheme Identifier` sub-field.

We therefore propose to create a new profile, called `Profile C`. The specifics of Profile C is not important per se, but we want it to be used to indicate that the SUCI procedure is part of the SUCI-AKA protocol. Profile C may otherwise be similar to either profile A or B. The UE can then trigger the SUCI-AKA protocol by invoking a SUCI procedure with Profile C.

5.1.2 The Need for a Challenge

We want to design a double challenge-response scheme, and then we need to have a challenge from the UE to the HN. The challenge may be a pseudo-random number, but the essential attributes are that it needs to be unpredictable, fresh and unique.

5.1.3 The Ephemeral ECIES Key-Pair

Let us denote the UE key-pair as (U, u), where U is the public key and u the private key. Correspondingly, the (long-term) HN key-pair is denoted (H, h). The ephemeral public key from the SUCI scheme is known to the UE to be fresh. It must also be unique and unpredictable, otherwise it would be a very poor key. That is, U has the properties required for a challenge. We shall not go into a cryptographic analysis of the properties of U. Suffice to say that if the key-pair (U, u) is predictable, then the security of ECIES is compromised. The U is ephemeral, generated on demand and used only once. Thus, uniqueness should be easily attained.

5.1.4 Overloading the Ephemeral Public Key

Within a $SUCI$ identifier, the U is encoded in the `Scheme output` field. Specifically, U is found in the sub-field `ECC ephemeral public key`. Thus, the SUCI scheme already provides us with "challenge" candidate. This is fortunate, since we then also have a suitable mechanism to forward the challenge to the HN. We note that the U is encoded as either a 256-bit or 264-bit field. It is thus larger than the $RAND$ issued by the HN in the 5G-AKA protocol. The response function, which in 5G is a HMAC-functions, will work fine with variable length input.

5.1.5 The ECIES Diffie-Hellman Secret

In Figure 2, we find that the Diffie-Hellman secret is known as the `Ephemeral shared key` (we denote it as *epsk*). It is only used internally in the SUCI scheme, and is shared between the UE and the HN. In our design, it will be included as a parameter in the derivation of K_{AUSF}.

5.1.6 The Existing Key Derivation Function for K_{AUSF}

The existing KDF interface is defined in Annex A.2 in TS 33.501 [16]. The KDF itself is defined in Annex B.2 in TS 33.220 [19], and is based on HMAC-SHA-256. The "UMTS AKA" functions to derive CK, IK and AK are defined in TS 33.105 [13].

$$A.2 : KDF_{(CK||IK)}(FC, P0, L0, P1, L1) \rightarrow K_{AUSF} \tag{2}$$

Where:

- CK, IK - Key-pair computed by "UMTS AKA" $f3_K(RAND)$) and $f4_K(RAND)$) function.
- FC - Function code. 0x6A for K_{AUSF}. Defined in TS 33.220 [19].
- P0 - Serving network name
- L0 - Length of P0
- P1 - $SQN \oplus AK$. The sequence number (masked by the anonymity key).
- L1 - Length of P1

5.1.7 The Proposed Alternative Key Derivation Function for K_{AUSF}

The modified KDF is modelled on the exiting A.2 function. We denote it $A.2'$. The sequence number SQN is not used by SUCI-AKA, and it is instead replaced by the *epsk* key. That is,

parameter $P1$ will be the *epsk* for $A.2'$. There also needs to be a new function code, FC, for the $A.2'$ function.

$$A.2' : KDF_{(CK||IK)}(FC, P0, L0, P1, L1) \rightarrow K_{AUSF} \tag{3}$$

Given that *epsk* is a DH secret, a K_{AUSF} derived by the $A.2'$ function will have the perfect forward secrecy property.

5.2 The Building Blocks of the SUCI-AKA Protocol

We now want to combine the SUCI scheme with the basics of the 5G-AKA protocol. There needs to be some changes, but we want to keep the 5G-AKA message exchange. What we need is to modify the 5G-AKA protocol to bind it to a SUCI challenge. We require that:

- The HN must be able to indicate to the UE that it responds to a SUCI-AKA challenge.
- The HN must provide a response to the SUCI-based challenge.
- The HN must bind the response to its own challenge.
- The UE must bind its response to both challenges.

5.2.1 Using the AMF to Indicate the SUCI-AKA Protocol

The term AMF is used to name a network function and the Authentication Management Field (AMF), which is included in the $AUTN$ parameter. We here only refer to AMF in $AUTN$.

The AMF is defined in Annex H in TS 33.102 [12], and it can be used by the HN to configure the authentication policy and parameters at the UE. Bits $[1 \ldots 7]$ is currently reserved for future standardization. It will therefore be possible to use the AMF to indicate that the challenge is a SUCI-AKA challenge if one wants to. A SUCI-AKA AMF indicator will permit the HN to confirm to the UE that the challenge is part of a SUCI-AKA exchange.

5.2.2 HN Response to the SUCI-challenge

The HN needs to respond to the UE challenge. We can achieve this by modifying the challenge $\{RAND,AUTN\}$ to include the response. One can then create a new challenge such that:

$$HNChallenge : (RAND, AUTN, RES_{UE})$$

The current $RES*$ response function is defined in Annex A.4 in in TS 33.501 [16]. The SUCI-AKA equivalent function has the same layout as Function 1, but with slightly modified parameters.

$$Resu_{(CK||IK)}(FC, P0, L0, P1, L1, P2, L2) \rightarrow RES_{UE} \tag{4}$$

The SUCI-AKA equivalent parameters (only the changed parameters is included):

- FC - Function code. **** A new code must be defined.*
- $P1$ - $RAND||U$. **** The SUCI-AKA modification is to concatenate $RAND$ with U.*
- $L1$ - Length of P1

For SUCI-AKA, there is no need for the SQN or the AMF-A anymore. If USIM modifications is permitted, one can make the HN challenge slightly shorter: $(RAND, AMF, RESU)$.

5.2.3 UE Response to the HN challenge

Similarly as to the HN response, we want the UE response to include the U. The simplest way is to re-use Function 4, but with a new function code.

$$Resh_{(CK||IK)}(FC, P0, L0, P1, L1, P2, L2) \rightarrow RES_{HN} \tag{5}$$

5.3 Outline of the SUCI-AKA Protocol

We define the $SUCI{-}AV$ as follows:

$$SUCI{-}AV = \{RAND, AUTN, RES_{UE}, K_{AUSF}, XRES_{HN}\}$$

The outline if for a HN-challenge that does not require USIM changes. With basis in the outline in Section 3.5, we define the SUCI-AKA sequence as:

— **Initial phase: Identity presentation and UE challenge**

1. UE: Generate $SUCI$.
   UE→SN: N1-message($SUCI$)
2. SN→HN: UEAuth_AuthRequest($SUCI$, SN-name)
3. HN: De-conceal $SUPI$. Save $epsk$ and U. Select auth.method.

— **Main phase: The remaining AKA sequence**

4. HN.UDM/ARPF: Generate $SUCI{-}AV$.
5. HN: UDM/ARPF→AUSF: UEAuth_GetResponse($SUCI{-}AV$,$SUPI$)
6. HN.AUSF:
   - $A.5' : (RAND, XRES_{UE}) \rightarrow XRES_{SN}$ (expected response to SN)
   - $A.6_{K_{AUSF}}(FC, SN{-}name, Len(SN{-}name) \rightarrow K_{SEAF}$ (no change)
7. HN.AUSF→SN.SEAF: UEAuth_AuthResponse($RAND, AUTN, RES_{UE}, XRES_{SN}$)
8. SN.SEAF→UE: NAS_AuthReq($RAND, AUTN, RES_{UE}$)
9. UE Verify and Respond.
   - UE.USIM: Verify $AUTN$ ("UMTS-AKA" part). Forward AKA output to ME.
   - UE.ME: Verify that computed RES_{UE} equals the received $XRES_{UE}$ (from HN).
   - UE.ME: Compute RES_{HN}
10. UE.ME→SN.SEAF: NAS_AuthResp(RES_{HN})
11. SN.SEAF: Verify UE response
    - Compute RES_{SN} from received RES_{HN}.
    - UE is deemed to be authenticated by SN.SEAF iff ($RES_{SN} = XRES_{SN}$).
12. SN.SEAF→HN.AUSF: UEAuth_AuthRequest(RES_{HN})
13. HN.AUSF: Successful authentication iff: ($RES_{HN} = XRES_{HN}$). Log the result.
14. HN.AUSF→SN.SEAF: UEAuth_AuthResponse($SUPI, K_{SEAF}$)

Subsequent to the 5G-AKA sequence, the SEAF and the AUSF has the necessary security context key material (K_{SEAF} and ($KAUSF$) respectively), and both has assurance of the UE. The K_{AUSF} was derived with $epsk$ as one of the inputs. It cannot be derived without the $epsk$.

Given that the UE challenge (the U) essentially is a nonce, the UE will have assurance that the HN is present during the SUCI-AKA protocol run. The SUCI-AKA is a "normal" mutual challenge-response protocol in this respect. That is, one now has mutual entity authentication between the UE and the SN. The has essentially the same assurance of the UE as it would have had for a normal 5G-AKA run. The UE, likewise, has 5G-AKA equivalent assurance of the SN.

5.4 Brief Analysis of the SUCI-AKA Protocol

5.4.1 Efficiency

Efficiency, as hinted at in the design criteria, is not a particularly important criteria. The SUCI-AKA protocol is run whenever the SUCI identification is to be used. Computationally, the number of asymmetric operations is the same as for SUCI + 5G-AKA. The other modifications is basically only to the input to MAC functions, and these impacts are negligible.

There are some extra fields, etc., to the messages, but while this would have been important for previous generations, the size of the messages matters little to 5G signalling. For instance, the coding of SUCI, which contains the ephemeral public key, would not have been permissible for the 3G/4G radio protocols. For 5G, this is not an issue.

The no. of round-trips is perhaps the most important concern, as it directly affects the propagation delays during initial registration. Given that one for initial registration will have to run SUCI, the number of messages and the round-trips are the same for SUCI + 5G-AKA as it is for SUCI-AKA.

Thus, from a performance perspective, running SUCI-AKA is more or less equivalent to running SUCI + 5G-AKA.

5.4.2 Concerning the Design Requirements

The SUCI-AKA protocol adheres to the design criteria and the security requirements found in Section 2. It also fulfills the requirements defined in this section. But, is the SUCI-AKA protocol secure? Specifically, we ask:

- Does it provide mutual entity authentication between UE and the HN?
- Does it provide perfect forward secrecy?

The cryptographic binding of the challenges and responses is fairly standard. The construction of a challenge-response based mutual entity authentication protocol is not new by itself. To quote Boyd, Mathuria and Stebila (Chapter 3.6 in [20]):

> To a large extent the problem of key establishment between two parties using symmetric cryptography seems to have been solved.

We thus feel confident that the mutual challenge-response part is sound. The "novel" part is the use of ECIES in the SUCI scheme, but ECIES is well-known and provided that the ephemeral key pair really is ephemeral, there should be no problem using the U as a nonce. The DH secret from ECIES provides the K_{AUSF} with the perfect forward secrecy property. The one point that may really undermine our confidence in the SUCI-AKA protocol is overall complexity of the protocol. This complexity isn't really due to SUCI-AKA protocol, but is inherited from the 5G-AKA protocol. Thus, the complexity is more or less unavoidable given our design criteria. The SUCI-AKA protocol is designed to be close to the 5G-AKA protocol, while yet providing mutual entity authentication and sounder basis for the key hierarchy. Thus, the SUCI-AKA protocol depend on the SUCI- scheme and 5G-AKA protocol being sound to begin with.

Formal verification is often seen as a requirement for new protocols. And, certainly, formal verification would seems like a natural next step concerning the development of SUCI-AKA. However, we concur with Gollmann that proofs are a "non-goal" of formal verification [21], and that the real benefit is to clarify the design and elucidate its workings.

5.4.3 Limitations of the SUCI-AKA Protocol Approach

The SUCI-AKA protocol relies on the SUCI scheme and on slightly modifying the 5G-AKA protocol. The SUCI-AKA protocol is therefore unavoidably a complex protocol, and it is not as elegant or intuitive as it could have been for a greenfield case.

Another point worth making, is that the SUCI-AKA protocol is primarily used when UE enters a new network. This is when the UE needs to use SUCI to identify itself, and when the SUCI-AKA protocol is naturally triggered. Subsequent to this, the preferred identifier for the UE will be the $5G{-}GUTI$. These cases do not lend themselves naturally to trigger the SUCI-AKA protocol, and extending the SUCI-AKA protocol in this direction will add considerable complexity. On the other hand, the importance of online mutual entity authentication between the UE and the HN is greatest for the cases where the UE enters a new network.

6 Summary and Conclusion

6.1 Summary

We have analysed the existing 5G-AKA protocol and found it to be wanting with respect to online mutual entity authentication. The 5G-AKA protocol is a product of an evolved system architecture and the lineage goes back to the analogue 1G systems.

A major contribution in 5G has been the inclusion of the SUCI procedure for concealed subscriber identifier presentation. SUCI is based on an ECIES scheme, and it provides credible identity privacy as well as location privacy for the subscriber. This is a major improvement. Curiously, the SUCI procedure and the 5G-AKA protocol seems to be seen as entirely independent procedures. Yet, the 5G-AKA will invariably be run subsequent to any SUCI invocation.

We have shown that if SUCI and 5G-AKA is seen as whole, only minor modifications is needed to provide an integrated solution. This new solution, which we call the SUCI-AKA protocol, provides full mutual entity authentication with only minor design modifications and virtually no run-time overhead. We note that it will be a matter of policy if and how often the UE should trigger a SUCI-AKA protocol run.

When the UE presents itself with $5G\text{-}GUTI$, the SUCI-AKA protocol will not be run. Thus, even with SUCI-AKA available, there will be cases where the 5G-AKA protocol will be run.

A topic for further study is to design a greenfield alternative AKA protocol. It may usefully include the SUCI basics, and it should likely retain the HN and SN anchor keys. Such protocol may not be realistic in the 5G context, but it may still be a worthwhile exercise.

6.2 Conclusion

In this paper we have demonstrated that one can achieve online mutual entity authentication in 5G by integrating the existing SUCI identity presentation scheme and 5G-AKA protocol. The changes needed to integrate the existing schemes into the SUCI-AKA protocol are rather minor, and that is in many ways the strength of the proposal.

A total redesign would very likely have afforded a simpler and more elegant scheme, while achieving at least the same security level. However, our goal was very much to provide a design that would co-exits with SUCI and 5G-AKA, and one which would accommodate the security requirements with the least impact on existing procedures. In this respect, we feel confident that the SUCI-AKA protocol is a worthy contribution. In short, it is a realistic design proposal with respect to the existing system architecture.

References

[1] Rosario Giustolisi, Christian Gehrmann, Markus Ahlström, and Simon Holmberg. A secure group-based aka protocol for machine-type communications. In *International Conference on Information Security and Cryptology*, pages 3–27. Springer, 2016.

[2] Khodor Hamandi, Imad Sarji, Ali Chehab, Imad H Elhajj, and Ayman Kayssi. Privacy enhanced and computationally efficient hsk-aka lte scheme. In *2013 27th International Conference on Advanced Information Networking and Applications Workshops*, pages 929–934. IEEE, 2013.

[3] Jacques Bou Bou Abdo, Hakima Chaouchi, and Mohammad Aoude. Ensured confidentiality authentication and key agreement protocol for eps. In *2012 Symposium on Broadband Networks and Fast Internet (RELABIRA)*, pages 73–77. IEEE, 2012.

[4] Geir M. Køien. Privacy enhanced mutual authentication in LTE. In *Wireless and Mobile Computing, Networking and Communications (WiMob), 2013 IEEE 9th International Conference on*, pages 614–621. IEEE, 2013.

[5] Jin Cao, Zheng Yan, Ruihui Ma, Yinghui Zhang, Yulong Fu, and Hui Li. Lsaa: A lightweight and secure access authentication scheme for both ues and mmtc devices in 5g networks. *IEEE Internet of Things Journal*, 2020.

[6] Ikram Gharsallah, Salima Smaoui, and Faouzi Zarai. A secure efficient and lightweight authentication protocol for 5g cellular networks: Sel-aka. In *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, pages 1311–1316. IEEE, 2019.

[7] David Basin, Jannik Dreier, Lucca Hirschi, Saša Radomirovic, Ralf Sasse, and Vincent Stettler. A formal analysis of 5g authentication. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 1383–1396, 2018.

[8] Jari Arkko, Karl Norrman, Mats Näslund, and Bengt Sahlin. A USIM compatible 5G AKA protocol with perfect forward secrecy. In *2015 IEEE Trustcom/BigDataSE/ISPA*, volume 1, pages 1205–1209. IEEE, 2015.

[9] 3GPP. TS 33.120 "3G security; Security principles and objectives", Rel.4.0, 03 2001.

[10] 3GPP. TS 23.003 "Numbering, addressing and identification", Rel.16.3, 07 2020.

[11] Víctor Gayoso Martínez, Luis Hernández Encinas, and Carmen Sánchez Ávila. A survey of the elliptic curve integrated encryption scheme. *Journal of Computer Science and Engineering (JCSE)*, 2:7–13, 08 2010.

[12] 3GPP. TS 33.102 "3G security; Security architecture", Rel.16.0, 07 2020.

[13] 3GPP. TS 33.105 "3G security; Cryptographic algorithm requirements", Rel.16.0, 07 2020.

[14] Valtteri Niemi and Kaisa Nyberg. *UMTS Security*. John Wiley & Sons, 2003.

[15] Geir M. Køien. An introduction to access security in UMTS. *IEEE Wireless Communications*, 11(1):8–18, 02 2004.

[16] 3GPP. TS 33.501 "Security architecture and procedures for 5G System", Rel.16.3, 07 2020.

[17] Anand R Prasad, Sivabalan Arumugam, B Sheeba, and Alf Zugenmaier. 3GPP 5G security. *Journal of ICT Standardization*, 6(1):137–158, 2018.

[18] 3GPP. TS 23.002 "Network architecture", Rel.16.0, 07 2020.

[19] 3GPP. TS 33.220 "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)", Rel.16.1, 07 2020.

[20] Colin Boyd, Anish Mathuria, and Douglas Stebila. *Protocols for Authentication and Key Establishment (2 ed.)*. Springer Nature, 2019.

[21] Dieter Gollmann. Analysing Security Protocols. In A.E. Abdalla, P. Ryan, and S. Schneider, editors, *Formal Aspects of Security*, volume 2629 of *LNCS*, pages 71–80, London, UK, 12 2002. Springer.